

Listing of Claims.

1. (Currently amended) A system for increasing data access in a secure socket layer network environment, which includes:

a web server computer having SSL protocol server software operably associated therewith for enabling a SSL connection, wherein SSL protocol server software includes a CA certificate and private key, SSL acceleration server software operably associated with said web server computer which includes a pseudo CA certificate and access to said private key and a public key; and

a client computer communicatively linked to said web server computer having web browser software having SSL protocol client software operably associated therewith for enabling a first SSL connection between said client and said web server, SSL acceleration client software operably associated with said client computer which communicates with said SSL acceleration server software to receive a copy of said pseudo CA certificate and said public key and present said pseudo CA certificate to said web browser software for validation thereof for enabling a second concurrent SSL connection between said client computer and said web server computer in a manner which permits optimization techniques to be applied on data transmitted through said second concurrent SSL connection.

2. (Previously presented) The system of claim 1, wherein said SSL acceleration client software is further equipped for monitoring when said web browser requests a SSL connection with said web server computer and intercepting said SSL request from said web browser, and diverting communication through one of an established and an initiated SSL connection through

said SSL acceleration client software and SSL acceleration server software.

3. (Previously presented) The system of claim 1, wherein said SSL acceleration client software is equipped to initiate a SSL request to said SSL acceleration server software operably disposed with web server computer to establish a SSL connection.

4. (Previously presented) The system of claim 3, wherein SSL acceleration server software is further equipped for monitoring when the web server computer receives a request for a SSL connection through said SSL acceleration client software where upon such request initiates a SSL handshake wherein said pseudo CA certificate is sent to said client computer via SSL acceleration client software with a public key.

5. (Previously presented) The system of claim 4, wherein said web browser software is equipped to send a list of available encryption algorithms to said web server computer and said SSL acceleration client software intercepts said list, selects an encryption algorithm from said list.

6. (Previously presented) The system of claim 5, wherein said SSL acceleration client software is equipped to send said chosen encryption algorithm to said browser software.

7. (Previously presented) The system of claim 6, wherein said browser software is equipped to create a secret key, encrypt using said chosen encryption algorithm and using said public key and send said encrypted secret key to said server computer through said SSL acceleration client software/ SSL acceleration server software.

8. (Previously presented) The system of claim 7, wherein said SSL acceleration server software is equipped to de-encrypt said secret key using said private key.

9. (Previously presented) The system of claim 1, which includes compression software for

transmitting data secure communications between said client computer and said web server computer over said second SSL connection.

10. (Currently amended) A system for increasing data access in a secure socket layer network environment, which includes:

a web server computer having a means for enabling a first SSL connection and SSL acceleration server software for transferring a copy of a pseudo CA certificate and a public key and permitting establishing a second concurrent SSL connection; and

a client computer communicatively linked to the web server computer having means for enabling said first SSL connection and having SSL acceleration client software operably associated with said client computer which communicates with said SSL acceleration server software to receive said copy of a pseudo CA certificate and said public key and present said pseudo CA certificate to web browser software on said client computer for validation thereof and for enabling said second concurrent SSL connection between said client computer and said web server computer in a manner which permits optimization techniques to be applied on data transmitted through said second concurrent SSL connection.

11. (Currently amended) A method for increasing data access in a secure socket layer network environment, which includes the steps of:

employing a web server computer having SSL protocol server software operably associated therewith for enabling a SSL connection, wherein SSL protocol server software includes a CA certificate and private key, SSL acceleration server software operably associated with said web server computer which includes a pseudo CA certificate and access to said private key and a public key; and

employing a client computer communicatively linked to said web server computer having web browser software having SSL protocol client software operably associated therewith for enabling a first SSL connection between said client and said web server, SSL acceleration client software operably associated with said client computer which communicates with said SSL acceleration server software to receive a copy of said pseudo CA certificate and said public key and present said pseudo CA certificate to said web browser software for validation thereof for enabling a second concurrent SSL connection between said client computer and said web server computer in a manner which permits optimization techniques to be applied on data transmitted through said second concurrent SSL connection.

12. (Previously presented) The method of claim 11, wherein said SSL acceleration monitors when said web browser requests a SSL connection with said web server computer and intercepts said SSL request from said web browser, and diverts communication through one of an established and an initiated SSL connection through said SSL acceleration client software and SSL acceleration server software.

13. (Previously presented) The method of claim 11, wherein said SSL acceleration client software initiates SSL request to said SSL acceleration server software web server computer to establish a SSL connection.

14. (Previously presented) The method of claim 13, wherein SSL acceleration server software monitors when the web server computer receives a request for a SSL connection through said SSL acceleration client software where upon such request initiates a SSL handshake wherein said pseudo CA certificate is sent to said client computer via SSL acceleration client software with a public key.

15. (Previously presented) The method of claim 14, wherein said web browser software sends a list of available encryption algorithms back to said web server computer through said SSL acceleration client software and SSL acceleration server software.
16. (Previously presented) The method of claim 15, wherein said SSL acceleration client software sends a chosen encryption algorithm to said browser.
17. (Previously presented) The method of claim 16, wherein said browser software creates a secret key, encrypts using said chosen encryption algorithm and using said public key and sends said encrypted secret key to said server computer through said SSL acceleration client software/SSL acceleration server software.
18. (Previously presented) The method of claim 17, wherein said SSL acceleration server software de-encrypts said secret key using said private key.
19. (Previously presented) The method of claim 11, which includes employing compression software for transmitting data secure communications between said client computer and said web server computer over said second SSL connection.
20. (New) The system of claim 1, wherein said concurrent SLL connections are direct connection between said client and said server.
21. (New) The system of claim 1, wherein said concurrent SLL connections are indirect connection between said client and said server.
22. (New) The system of claim 10, wherein said concurrent SLL connections are one of direct and indirect connection between said client and said server.
23. (New) The method of claim 11, wherein said concurrent SLL connections are one of direct and indirect connection between said client and said server.